

19/7/6

DIALOG(R)File 347:JAPIO

(c) 2002 JPO & JAPIO. All rts. reserv.

06745083 **Image available**

INTRANET SYSTEM AND METHOD FOR CONTROLLING *SERVER*

PUB. NO.: 2000-330937 [JP 2000330937 A]

PUBLISHED: November 30, 2000 (20001130)

INVENTOR(s): SHINKAWA TARO

APPLICANT(s): YASKAWA ELECTRIC CORP

APPL. NO.: 11-136187 [JP 99136187]

FILED: May 17, 1999 (19990517)

ABSTRACT

PROBLEM TO BE SOLVED: To easily increase the scale of the *intranet* system and the capacity of contents while maintaining fast access to a representing *server* by providing proxy *servers* between the representing *server* and a terminal device and decentralizing *authenticating* and access control processes for *users*.

SOLUTION: When a request to browse desirable contents is sent to a proxy *server* 11 by using the terminal device 13 of a user 15, the proxy *server* 11 having received the request retrieves the user. Then it is judged whether authentication and access control information on the user is already registered on the proxy *server* 11. When the user 15 always makes requests to browse contents through a terminal device 13 under the proxy *server* 11, the *authentication* and access control information on the *user* 15 is stored in the proxy *server* 11, so it is speedily judged whether or not browsing is allowed; when browsing is allowed, the contents are immediately sent to the terminal device 13 of the user 15 from a representing *server* 10 and when not, it is immediately informed that the use is disallowed.

COPYRIGHT: (C)2000,JPO

19/7/7

DIALOG(R)File 347:JAPIO

(c) 2002 JPO & JAPIO. All rts. reserv.

06623473 **Image available**

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-330937
(P2000-330937A)

(43)公開日 平成12年11月30日(2000.11.30)

(51)Int.Cl. ⁷	識別記号	F I	テーム(参考)
G 0 6 F 15/00	3 1 0	G 0 6 F 15/00	3 1 0 A 5 B 0 7 5
	3 3 0		3 3 0 B 5 B 0 8 5
13/00	3 5 1	13/00	3 5 1 Z 5 B 0 8 9
17/30		15/40	3 1 0 F
			3 2 0 B

審査請求 未請求 請求項の数2 O L (全 6 頁)

(21)出願番号 特願平11-136187

(22)出願日 平成11年5月17日(1999.5.17)

(71)出願人 000006622

株式会社安川電機

福岡県北九州市八幡西区黒崎城石2番1号

(72)発明者 新川 太郎

福岡県北九州市八幡西区黒崎城石2番1号

株式会社安川電機内

Fターム(参考) 5B075 KK02 KK43 KK63

5B085 AE23 BG07

5B089 GA11 GA19 HA10 JA22 KA06

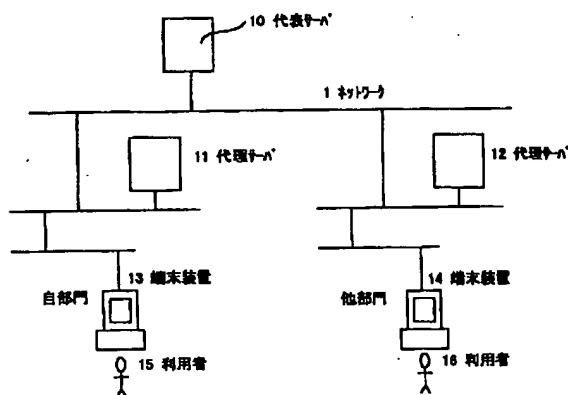
KA17 KB13 KC44 KC58 MA03

(54)【発明の名称】 イン트라ネットシステム及びサーバの制御方法

(57)【要約】

【課題】 イン트라ネットの大規模化とサーバのコンテンツの大容量化を可能にする。

【解決手段】サーバと端末装置がネットワーク1で接続されたイントラネットシステムに、端末装置13から閲覧可能な情報を格納した代表サーバ10と、利用者15が端末装置13を用いて代表サーバ10の情報を閲覧する時は、その閲覧要求を受けて利用者15の認証をし、認証にパスしたら閲覧要求された情報が利用可能かどうかを判断し、利用可能であれば代表サーバ10に情報の提供を要求し、利用可能でない場合と認証にパスしない場合はその旨利用者15に伝える代理サーバ11とを備える。



【特許請求の範囲】

【請求項 1】サーバと端末装置とがネットワークを介して接続されたイントラネットシステムにおいて、前記端末装置から閲覧可能な情報を格納した代表サーバと、

利用者が前記端末装置を用いて前記代表サーバの情報を閲覧する時は、その閲覧要求を受けて利用者の認証をし、認証にパスしたら閲覧要求された情報が利用可能かどうかを判断し、利用可能であれば前記代表サーバに情報の提供を要求し、利用可能でない場合と認証にパスしない場合はその旨利用者に伝える代理サーバとを備えたことを特徴とするイントラネットシステム。

【請求項 2】代表サーバと代理サーバと端末装置とがネットワークを介して接続されたイントラネットシステムにおいて、前記代表サーバと前記代理サーバとが次の処理を行うよう制御されることを特徴とするサーバの制御方法。

(1) 代理サーバが利用者の閲覧要求を受けると、利用者検索をする。

(2) 代理サーバは、利用者の認証・アクセス制御情報が代理サーバに登録済みかどうかを判断する。登録済みの場合は(3)に移行し、そうでない場合は(5)に移行する。

(3) 代理サーバは要求された情報が閲覧可能かどうかを検査し、可能であれば

(4)に移行し、可能でなければ(9)に移行する。

(4) 代表サーバが情報を利用者の端末装置に送り、処理を終了する。

(5) 代理サーバが代表サーバに利用者の認証・アクセス制御情報を要求して受けとり、代表サーバが利用者の認証・アクセス制御情報の所在情報を検査する。

(6) 代表サーバに代理サーバの、利用者の認証・アクセス制御情報の所在情報があるかどうかを判断し、ない場合は(7)に移行し、ある場合は(8)に移行する。

(7) 代表サーバが利用者の認証・アクセス制御情報の所在情報を格納して(3)に移行する。

(8) 代表サーバが代理サーバに指示して利用者の認証・アクセス制御情報を破棄させ、(7)に移行する。

(9) 代理サーバが利用者にパスワードを入力させて認証情報と比較する。

(10) 利用者の認証にパスすれば(4)に移行し、パスしなければ(11)に移行する。

(11) 代理サーバは情報を閲覧できないことを利用者に伝え、処理を終了する。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、組織内で利用されるイントラネットサーバの認証とアクセス制御の負荷を分散させ、サーバへのアクセスを高速化するイントラネットシステムとサーバの制御方法に関する。

【0002】

【従来の技術】情報伝達の速さや、情報の共有など多くの利点から企業などの組織体でイントラネットが普及しつつある。その接続形態は図7に示すように、イントラネットサーバ70がネットワーク1を介して多数の端末装置71、72、73、73…に接続されるというものである。イントラネットサーバ70には様々な情報が格納されており、ブラウザを使って端末装置71、72、73、73…から閲覧することができるようになっている。イントラネットサーバ70に格納されている情報には、人事情報や、財務情報、各種の報告書類等、無差別には公開されていない特定の情報もあり、アクセス制限が施されている。利用者がそれらの情報を閲覧する際は、イントラネットサーバ70が利用者の認証を行い、その後、閲覧許可のある情報だけを提供するというアクセス制御処理をしている。こうして、閲覧可能な情報だけが閲覧許可のある利用者に提供されるようになっている。

【0003】

【発明が解決しようとする課題】ところが、イントラネットが大規模になり、端末装置の数とイントラネットサーバに蓄積する情報の量が増えてくると、利用者の認証とアクセス制御を行うイントラネットサーバの負荷が増大し、アクセスする際の所用時間が著しく長くなったり、接続がうまく行かなくなったりすることが多発するなど、イントラネットの利用状況に重大な影響を与えるようになっている。これを回避するには、いっそう高性能なイントラネットサーバの導入が必要となり、コストアップを招いていた。

【0004】

【課題を解決するための手段】上記問題を解決するため、本発明は、サーバと端末装置とがネットワークを介して接続されたイントラネットシステムにおいて、前記端末装置から閲覧可能な情報を格納した代表サーバと、利用者が前記端末装置を用いて前記代表サーバの情報を閲覧する時は、その閲覧要求を受けて利用者の認証をし、認証にパスしたら閲覧要求された情報が利用可能かどうかを判断し、利用可能であれば前記代表サーバに情報の提供を要求し、利用可能でない場合と認証にパスしない場合はその旨利用者に伝える代理サーバとを備えたことを特徴としている。また本発明のサーバの制御方法は、代表サーバと代理サーバと端末装置とがネットワークを介して接続されたイントラネットシステムにおいて、前記代表サーバと前記代理サーバとが次の処理を行うよう制御されることを特徴とするサーバの制御方法。

(1) 代理サーバが利用者の閲覧要求を受けると、利用者検索をする。

(2) 代理サーバは、利用者の認証・アクセス制御情報が代理サーバに登録済みかどうかを判断する。登録済みの場合は(3)に移行し、そうでない場合は(5)に移

行する。

(3) 代理サーバは要求された情報が閲覧可能かどうかを検査し、可能であれば(4)に移行し、可能でなければ(9)に移行する。

(4) 代表サーバが情報を利用者の端末装置に送り、処理を終了する。

(5) 代理サーバが代表サーバに利用者の認証・アクセス制御情報を要求して受けとり、代表サーバが利用者の認証・アクセス制御情報の所在情報を検査する。

(6) 代表サーバに代理サーバの、利用者の認証・アクセス制御情報の所在情報があるかどうかを判断し、ない場合は(7)に移行し、ある場合は(8)に移行する。

(7) 代表サーバが利用者の認証・アクセス制御情報の所在情報を格納して(3)に移行する。

(8) 代表サーバが代理サーバに指示して利用者の認証・アクセス制御情報を破棄させ、(7)に移行する。

(9) 代理サーバが利用者にパスワードを入力させて認証情報と比較する。

(10) 利用者の認証にパスすれば(4)に移行し、パスしなければ(11)に移行する。

(11) 代理サーバは情報を閲覧できないことを利用者に伝え、処理を終了する。

【0005】

【発明の実施の形態】以下、本発明の実施の形態を図に基づいて説明する。図1は本発明のイントラネットシステムの接続形態を示す図であり、図2はその補足説明図、図3、図4、図5はそれぞれ代表サーバと代理サーバ、端末装置の構成を示す図である。図1、図2において、1はネットワーク、10、20は代表サーバ、11、12、21、22は代理サーバ、13、14、23、24は端末装置、15、16、25は利用者である。代理サーバ11、12、21、22は、部門サーバなど、他の機能を兼ねる計算機であっても良いし、パソコン等の利用者端末を代用しても良い。

【0006】図3において、代表サーバは記憶装置30と演算装置31、通信装置32とを備えており、記憶装置30にはコンテンツ33、コンテンツアクセス制御データベース34、ユーザ認証用データベース35、ユーザ認証情報所在データベース36が格納されている。コンテンツ33は利用者が閲覧することができる情報、コンテンツアクセス制御データベース34はコンテンツ33が閲覧可能かどうかの情報を含むデータベース、ユーザ認証用データベース35はユーザの認証に使われる情報を含むデータベース、ユーザ認証情報所在データベース36はユーザ認証情報がどこにあるかという情報を含むデータベースである。通信装置32はネットワーク1と演算装置31に接続されており、ネットワーク1を介して外部の機器と通信する機能を有している。演算装置31は、情報の入出力や認証などの制御をする機能を有している。ネットワーク1と通信装置32を使って代理

サーバと通信するときは、記憶装置30のコンテンツアクセス制御データベース34、ユーザ認証用データベース35、ユーザ認証情報所在データベース36を参照して通信制御し、コンテンツ33を送信して良いと判断したときは通信装置32に送信指令を与える。

【0007】代理サーバ11は記憶装置40と演算装置41、通信装置42とを備えており、記憶装置40にはコンテンツアクセス制御データベースキャッシュ43、ユーザ認証用データベースキャッシュ44が格納されている。コンテンツアクセス制御データベースキャッシュ43は代表サーバのコンテンツ33がアクセスされる際に参照されるキャッシュ、ユーザ認証用データベースキャッシュ44はユーザの認証をする際に参照されるキャッシュである。通信装置42はネットワーク1と演算装置41に接続されており、ネットワーク1を介して外部の機器と通信する機能を有している。演算装置41は、情報の入出力や認証などの制御をする機能を有している。ネットワーク1と通信装置42を使って代表サーバ及び端末装置と通信するときは、コンテンツアクセス制御データベースキャッシュ43とユーザ認証用データベースキャッシュ44を参照して通信制御し、代表サーバにコンテンツ33の送信の可否を伝える機能を有している。

【0008】端末装置13は記憶装置50と演算装置51、通信装置52とを備えており、記憶装置50には汎用ブラウザソフトウェア53が格納されている。汎用ブラウザソフトウェア53は代表サーバのコンテンツ33を閲覧する機能を備えたツールである。通信装置52はネットワーク1と演算装置51に接続されており、ネットワーク1を介して外部の機器と通信する機能を有している。演算装置51は、情報の入出力や認証の要求をする機能を有している。汎用ブラウザソフトウェア53が起動すると、ネットワーク1と通信装置52を使って代理サーバで認証を受け、認証にパスしてコンテンツ33が閲覧可能であればコンテンツ33を受信して閲覧することができる。

【0009】図1の接続形態をしたイントラネットシステムで利用者15が代表サーバ10に格納されている情報を閲覧するときは、イントラネットシステムは図6のフローチャートに沿って動作する。この図において、まず(S1)で利用者15が端末装置13を使って代理サーバ11に閲覧したいコンテンツ33の閲覧要求をする、(S2)で閲覧要求を受けた代理サーバ11が利用者の検索をする。そして(S3)で代理サーバ11は利用者の認証・アクセス制御情報が代理サーバ11に登録済みかどうかを判断し、登録済みであれば(S4)に移行して、そうでなければ(S7)に移行する。(S4)では代理サーバ11が、代表サーバ10のコンテンツ33が参照可能かどうかを検査する。その結果、(S5)利用者が代表サーバ10のコンテンツ33を閲覧するこ

とが可能と判断されれば(S6)に移行し、そうでなければ(S14)に移行する。(S7)では代理サーバ11が代表サーバ10に利用者15の認証・アクセス制御情報を要求し、(S8)その要求を受けた代表サーバ10が代理サーバ11に利用者15の認証・アクセス制御情報を伝え、同時に(S9)利用者15の認証・アクセス制御情報の所在情報を検索する。そして(S10)代表サーバに代理サーバの利用者15の認証・アクセス制御情報の所在情報がなければ(S13)に移行し、そうでなければ(S11)に移行する。(S11)では、代表サーバ10は利用者15の認証・アクセス制御情報を破棄するよう代理サーバ11に通知し、(S12)代理サーバ11が該当する情報を破棄して(S13)に移行する。(S13)では、代表サーバ10は利用者15の認証・アクセス制御情報の所在情報を記憶装置30に格納して(S4)に移行する。(S14)では、代理サーバ11が利用者15の認証をし、(S15)認証にパスしたと判断したら(S6)に移行し、そうでなければ(S16)に移行する。(S16)では、代理サーバ11は、利用者15が使っている端末装置13に、利用者15が代表サーバ10のコンテンツ33を閲覧できないということを通知して、処理を終了する。(S6)では、代表サーバ10がコンテンツ33を利用者15が使っている端末装置13に送信して処理を終了する。

【0010】上記の手順でイントラネットシステムが動作しているため、利用者15が常に代理サーバ11の下位にある端末装置13でコンテンツ33の閲覧要求をするときは、利用者15の認証・アクセス制御情報が代理サーバ11に格納されているので、代理サーバ11で閲覧の可否が速やかに判断され、閲覧可能な場合はすぐに代表サーバ10からコンテンツ33が利用者15の端末装置13に送信され、そうでない場合は利用できないことがすぐに通知される。また、図2のように、利用者25が通常とは異なる代理サーバ22の下位にある端末装置24を使って閲覧要求をするときは、代理サーバ22が代表サーバ20から利用者25のユーザ認証所在情報を得るとともに、代表サーバ20が代理サーバ21に蓄えられている利用者25の認証・アクセス制御情報を廃棄させるので、認証・アクセス制御情報を速やかに書き換えることができ、閲覧可能かどうかの判断も速やかに行うことができるのである。

【0011】このように、代表サーバの下位にある全ての利用者の認証・アクセス制御情報が代表サーバで一元管理されているとともに、利用者が同じ代理サーバを使

って閲覧要求をする限り、その代理サーバによって全ての認証・アクセス制御が行われる。上記のほか、代表サーバで管理されている利用者の認証・アクセス制御情報に変更があった場合には、直前に認証作業をした代理サーバが蓄積している利用者の認証・アクセス制御情報が更新され、最新の認証・アクセス制御情報が保持される。

【0012】

【発明の効果】以上述べたように、本発明によれば、代表サーバと端末装置の間に複数の代理サーバを設けてユーザの認証・アクセス制御処理を分散させ、代表サーバに認証・アクセス制御情報の一元管理をさせているので、代表サーバへのアクセスの高速性を維持しつつイントラネットシステムの大規模化とコンテンツの大容量化を容易にすることができるという実用的効果がある。

【図面の簡単な説明】

【図1】 本発明のイントラネットシステムの接続形態図

【図2】 補足説明図

20 【図3】 代表サーバの構成図

【図4】 代理サーバの構成図

【図5】 端末装置の構成図

【図6】 本発明の処理手順を示すフローチャート

【図7】 従来のイントラネットシステムの接続形態図

【符号の説明】

1 ネットワーク

10、20 代表サーバ

11、12、21、22 代理サーバ

13、14、23、24、71、72、73、74 端末装置

15、16、25 利用者

30、40、50 記憶装置

31、41、51 演算装置

32、42、52 通信装置

33 コンテンツ

34 コンテンツアクセス制御データベース

35 ユーザ認証用データベース

36 ユーザ認証情報所在データベース

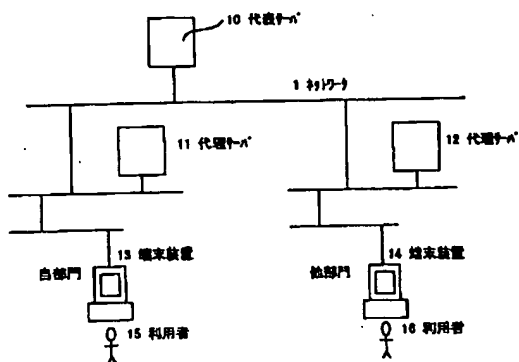
43 コンテンツ・アクセス制御データベースキャッシュ

44 ユーザ認証用データベースキャッシュ

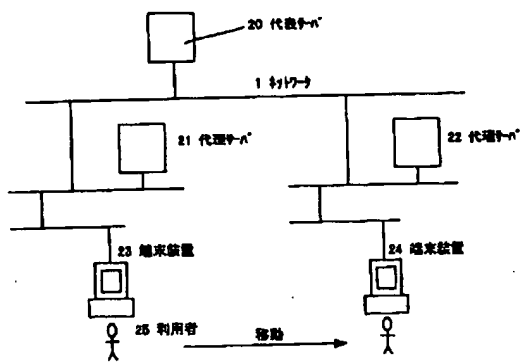
53 汎用ブラウザソフトウェア

70 イントラネットサーバ

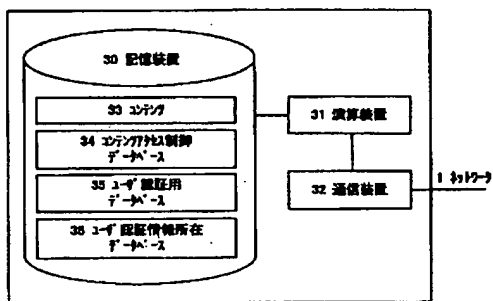
【図1】



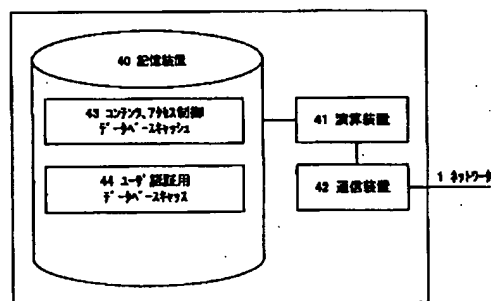
【図2】



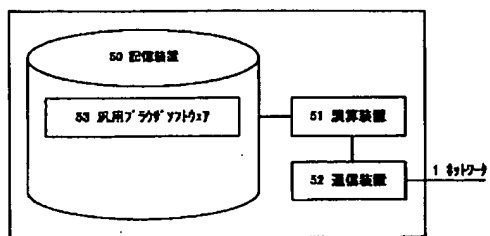
【図3】



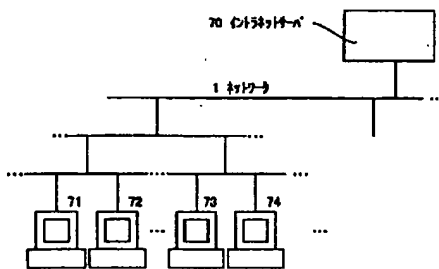
【図4】



【図5】



【図7】



【図6】

